Final

BULLETIN NO. 2004-09		**Date: February 27, 2004**
U.S. Department of Labor Employment and Training Administration Office of Apprenticeship Training, Employer and Labor Services (OATELS) Washington, D.C. 20210	Distribution: A-541 National Office A-546 All Field Tech A-547 SD+RD+SAC+; Lab.Com	Code: 200 Subject: New Apprenticeable Occupation – Information Assurance (IA) Specialist
Symbols: DSNIP/WC		Action: Immediate

PURPOSE: To inform the OATELS and Bureau of Apprenticeship and Training Staff (BAT)of a new apprenticeable occupation:

> IA Specialist
> RAIS Code: 1060
> O* NET Code: 15-1071.01
> Training Term: 6000 hours OJL, 1050 hours Related Instruction

Note: The Office of Policy Development Evaluation and Research no longer includes the issuance of Dictionary of Occupational Title Codes.

BACKGROUND:

Washington State Director Anne Wetmore, on behalf of the Naval Undersea Warfare Center, Division Keyport, WA, initiated this apprenticeability request for this occupation.

The specific requirements for completing the IT Generalist concentration are:

1) 6000 hrs of on-the-job learning through an approved employer sponsor,
2) 1050 hrs of (OJL) ILT in IT technical training as defined in the standards,

ACTION:

All OATELS staff should review and retain a copy of this bulletin, including all attachments, as a source for developing apprenticeship standards and/or providing technical assistance.

Attachments

APPRENTICEABILITY DETERMINATION FOR THE OCCUPATION:

Information Assurance Specialist
ONET # 15-1071.01
Originally Submitted by ATELS WA State Director Anne Wetmore, May 19, 2003
Resubmitted March 11, 2004

**PROGRAM SPONSOR: *NAVAL UNDERSEA WARFARE CENTER
DIVISION KEYPORT, WASHINGTON***

OCCUPATION: INFORMATION ASSURANCE SPECIALIST

Definition: An information assurance specialist provides planning, analysis, development, implementation, upkeep, and enhancement of systems, programs, policies, procedures and tools to ensure the integrity, reliability, accessibility, and confidentiality of information systems and assets. It includes information assurance functions that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. An information assurance specialist also provides for the restoration of information systems by incorporating protection, detection, and reaction capability. This includes system/network protection; intrusion detection and monitoring; readiness assessments; firewall administration; security policy enforcement; risk and vulnerability assessments; security evaluations and audits; and contingency plans and disaster recovery procedures.

 Three Levels of IAS Apprenticeship:

Technician I--- 2,000 hours on-the-job training plus 350 hours of related classroom

Technician II—2,000 hours on-the-job training plus 350 hours of related classroom

Technician III--2,000 hours on-the-job training plus 350 hours of related classroom

TOTAL TERM of APPRENTICESHIP:

6,000 hours OJT plus 1050 hours classroom and 3 Industry Certifications

(Management IAS Levels I, II, and III – To be developed later)

This sponsor has presented their paper entitled, "Developing Information Assurance Workers through Apprenticeship" to the 2003 Colloquium for Information Systems and Security Education Conference sponsored by the Executive Branch of the US Government, Critical Information Assurance Office, National Security Agency, and others held on June 2-4, 2003.

This occupation falls both under Information Technology and Homeland Security.

This trade schedule supplement, work processes are as follows, including work process, description, competencies, and estimated hours required:

Following the trade schedule is the related instruction schedule.

TRADE SCHEDULE FOR:
INFORMATION ASSURANCE

This trade schedule supplement, work process, is attached to and a part of the Apprenticeship Standards for the above identified occupation.

During the term of apprenticeship, the Apprentice shall receive such instruction and experience, in all branches of the occupation, as is necessary to develop a practical and versatile worker. Major processes in which Apprentices will be trained (although not necessarily in the order listed) and approximate hours (not necessarily continuous) to be spent in each are as follows:

Information Assurance Apprentice Technician Level 1					
Information Assurance Specialization - General (IA1 1.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA1 1.1	**Know:**	The "language" of security - **terms and acronyms**.			Ability to understand and explain security and Information Assurance terminology.
	Do:	Study and learn security terminology and common security acronyms.	4		
	ILT:	_			
	Exit:	Ability to understand and explain security and Information Assurance terminology.			
IA1 1.2	**Know:**	The roles and responsibilities of the **Information Assurance Organization.**			Ability to explain and discuss the IA organizational titles, roles and responsibilities.
	Do:	Correctly identify the IT organization structure, roles and responsibilities including roles such as; System Administrator, Information Assurance Manager, Information Assurance Officers, Network Security Manager, Network Security Officers, and Designated Approval Authority. Provide a complete and accurate short presentation or paper on the organization's security roles and responsibilities.	24		
	ILT:	_			
	Exit:	A complete and accurate short presentation or paper on the organization's security roles and responsibilities.			
IA1 1.3	**Know:**	**Password Security Concepts**			Ability to configure password characteristics for a domain.
	Do:	Become familiar with password policy and characteristics (length, complexity, age, etc…) associated with domains.	16		
	ILT:				
	Exit:	Demonstrate the ability to configure password characteristics for a domain.			

IA1 1.4	**Know:**	Common information **security risks and threats**.			Ability to explain, discuss and communicate the importance of Information and Systems security including common risks, threats and vulnerabilities.
	Do:	Review, discuss and learn the importance of Information Systems Security. Understand the importance of protection mechanisms.	4		
	ILT:	Information Age Technology", "Federal Information Systems Security Awareness", "Computer Security 101", "Protect your AIS", Protect your AIS, the Sequel", "Networks at Risk", "Identity Theft: Protect Yourself" (WBT) Videos; http://certifiedtechtrainers.com/Advanced%20Security%20Essentials.htm		4	
	Exit:	Completion of video training and a monitored discussion with organization security personnel on the importance of IT security practices.			
IA1 1.5	**Know:**	Organization's **security policies** and practices**.**			Ability to discuss, explain and communicate organizational security policies and practices and supporting rationale.
	Do:	Identify the organization's security policy and practices and how they combine to implement due care and due diligence within an organization. Develop a short presentation or paper to a security audience demonstrating a working knowledge of the organization's security policies and practices.	16		
	ILT:				
	Exit:	A short paper or presentation to a security audience demonstrating a working knowledge of the organization's security policies and practices.			
IA1 1.6	**Know:**	Organizational **security ethics** and federal ethics statutes.			Ability to explain, discuss and communicate the organization's security ethics policies and fundamental federal security statutes.
	Do:	Demonstrate a working knowledge of the organization's security ethics, applicable National security ethics, statutes and organizations acceptable use policy. Provide a short presentation to a group on security ethics of the organization.	8		
	ILT:				
	Exit:	A short presentation to a group on security ethics of the organization and federal statutes.			
IA1 1.7	**Know:**	Overview of areas of **IA specialization career fields**, as seen from a career development standpoint.			Ability of see individual IA career path.
	Do:	Review, research and discuss an understanding of specific IA career paths and begin to identify what path(s) are of greatest interest.	16		
	ILT:				
	Exit:	Identification of general career interests.			

			Hours		Job Related Competencies

	Know:	The organization's data **classification levels,** system roles, and criteria.			Ability to explain, discuss and communicate the organization's information classification system roles, classes and criteria.
IA1 1.8	**Do:**	Review, research and discuss how the organizations classification structure functions.	16		
	ILT:				
	Exit:	Successfully preform in-box exercise demonstrating proper data classification levels.			
	Know:	**Basic Security and QA.**			Ability to develop a sound testing strategy and implement the strategy against an application.
IA1 1.9	**Do:**	Develop a sound testing strategy and implementing the strategy against an application including identification, tracking and communication of bugs found with developer.	24		
	ILT:				
	Exit:	End User and developer acceptance of program and components.			
	Know:	Unique and specific aspects relating to organizations **Internal Security.**			Ability to maintain the organizations internal security domain.
IA1 1.10	**Do:**	Review, research and discuss significant internal security threats and potential mitigations.	24		
	ILT:	Operations Security Technology		40	
	Exit:	Provide a discussion paper on a significant internal security threat and potential mitigations.??			
	Know:	**Carnegie Melon Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework.**			Ability to focus on how operational systems are used to conduct an organization's business.
IA1 1.11	**Do:**	Review, research and discuss purpose, key concepts and three phases of the OCTAVE model developed by Carnegie Mellon University.	8		
	ILT:	Risk Assessment Basics		40	
	Exit:	Successfully evaluate the organizations security risks in an operational context.			
	Know:				
IA1 1.12	**Do:**				
	ILT:				
	Exit:				

Information Assurance Specialization - Network (IA1 2.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
	Know:	**Network troubleshooting** techniques.			Ability to resolve network problems using software tools.
IA1 2.1	**Do:**	Using basic tools such as ping, trace and others to isolate and repair a network problem.	80		
	ILT:	Networking I		40	
	Exit:	Successfully resolve problems using software tools.			

IA1 2.2	**Know:**	Concepts and functions of **Virtual Private Networking.**			Ability to secure an organizations VPN.
	Do:	Configure client and VPN gateway for secure authentication and encryption.	80		
	ILT:	Network Security Basics		40	
	Exit:	Successfully and independently configure client and VPN gateway for secure authentication and encryption.			
IA1 2.3	**Know:**	Understanding the more **advanced router administration** functions and their interrelations.			Ability to support an organizations router administration.
	Do:	Configure routers, switches and other network components and put them to work in the network.	80		
	ILT:	Networking II		40	
	Exit:	Successfully and independently configure routers, switch and other network components.			
IA1 2.4	**Know:**	Layers 1-4 of the OSI model and **securing the network backbone.**			Ability to troubleshoot the backbone and keep the network secure.
	Do:	Troubleshoot the backbone. Understand router and switch protocol. Determine subtle difference between normal and abnormal functions. TACACS	80		
	ILT:	Networking III		40	
	Exit:	Successfully provide network troubleshooting, identification of normal and abnormal functioning. Identify when to suspect a bug in IOS code.			
IA1 2.5	**Know:**	A basic understanding of the **organizations network layout**, technologies used, key hubs or routing centers, etc.			Ability to understand of the organizations network technologies and topologies
	Do:	Study existing documenation and discuss the network architecture with local networking personnel.	40		
	ILT:				
	Exit:	Create a high level network drawing showing the 3 tier network architecture of the network.			
IA1 2.6	**Know:**	Procedures of **Network Documentation.**			Ability to read and revise physical network topology diagrams.
	Do:	Use network documentation to find subnets in buildings, fiber runs from building to building and network devices used in each building.	80		
	ILT:				
	Exit:	Successfully document physical network topology diagrams, using drawing and spreadsheets.			
IA1 2.7	**Know:**	Practices and procedures for **network services back-up and recovery**.			Ability to perform network services

			OJL	ILT	
	Do:	Execute successful network services back-ups and recoveries. Validate that back-ups work properly in a lab environment.	24		back-ups and recoveries.
	ILT:				
	Exit:	Execute successful network services back-ups and recoveries.			
IA1 2.8	**Know:**	Basic operational concepts of **Internet Protocols** and the Internet.			Ability to explain basic operational concepts of Internet Protocols
	Do:	Complete training and discuss observations. Provide a demonstration of basic knowledge.	4		
	ILT:	"Warriors of the Net"		1	
	Exit:	Completion of training and a demonstration of basic knowledge.			

			Hours		Job Related Competencies
Information Assurance Specialization - Services (IA1 3.1)			OJL	ILT	
IA1 3.1	**Know:**	Practices and procedures for user **account management** and access privileges.			Ability to establish, update and disestablish user accounts and access privileges.
	Do:	Successfully demonstrate the ability to maintain user accounts and access privileges. Participate in establishing, updating and disestablishing user accounts and access privileges (infrastructure access pass-words, account rights, system level pass-words, strong pass-words, etc.)	24		
	ILT:				
	Exit:	Successfully demonstrate the ability to maintain user accounts and access privileges.			
IA1 3.2	**Know:**	The software and procedures employed to properly **install and configure Windows 2000 and Windows NT Server** computers.			Ability to install and properly configure Windows 2000 and Windows NT Server computers.
	Do:	Successfully complete W2k Baseline following the configuration document. Correctly configure a high-threat (e.g. DMZ) server.	80		
	ILT:				
	Exit:	Successfully and independently configure & secure a server.			
IA1 3.3	**Know:**	Understand the vulnerabilities and security configuration options of Microsoft Internet Explorer web browser.			Ability to install and properly configure Microsoft Internet Explorer.
	Do:	**Securely configure Microsoft Internet Explorer.**	40		
	ILT:				
	Exit:	Successfully and independently configure Microsoft Internet Explorer.			
IA1 3.4	**Know:**	Various technologies to provide **Security support for PED's.**			Ability to provide security for

			Hours		Job Related Competencies
	Do:	Configure and troubleshoot PDA, cell phones, etc. research, discuss and learn best practices.	40		PED's.
	ILT:				
	Exit:	Provide a discussion paper on significant PED security threat.			
IA1 3.5	**Know:**				
	Do:				
	ILT:				
	Exit:				

Information Assurance Specialization - Operations and Applications (IA1 4.1)			Hours		Job Related Competencies
			OJL	**ILT**	
IA1 4.1	**Know:**	Customer requirements and develop a backup strategy to meet identified requirements - with emphasis on **data base and application software security risks.**			Ability to understand application architecture security risks.
	Do:	Develop a backup strategy based on customer requirements and demonstrate a successful recovery within times identified in requirements.	80		
	ILT:				
	Exit:	Successfully and independently develop a backup strategy based on customer requirements and demonstrate a successful recovery within times identified in requirements			
IA1 4.2	**Know:**	**Security Operating Systems (LINUX, UNIX, Sun OS, Windows).**			Ability to install and configure an secure operating system.
	Do:	Install, properly configure and patching an operating system on a server in the IT test bed.	80		
	ILT:				
	Exit:	Successfully and independently install, properly configure and patching an operating system on a server in the IT test bed. The server must pass a security vulnerability scan. Provide a briefing on the security difference between systems.			
IA1 4.3	**Know:**				
	Do:				
	ILT:				
	Exit:				

Information Assurance Specialization - Practices (IA1 5.1)			Hours		Job Related Competencies
			OJL	**ILT**	
IA1 5.1	**Know:**	Software installation, configuration, and trouble shooting. Know how to provide file security and screen saver password support for **secure desktop systems.**			Ability to provide security for desktop systems.

			Hours		Job Related Competencies
	Do:	Use various technologies to provide security to the desktop system.	80		
	ILT:				
	Exit:	Provide a discussion paper on significant desktop operating system vulnerability supported by security scan.			
IA1 5.2	**Know:**	Basic understanding of how to create and **manage User Domain and Local system accounts.**			Ability to provide secure User Account Management.
	Do:	Create, modify and delete both domain and local system accounts.	40		
	ILT:				
	Exit:	Successfully and independently provide secure User Account Management.			
IA1 5.3	**Know:**				
	Do:				
	ILT:				
	Exit:				

			Hours		Job Related Competencies
Information Assurance Specialization - Tools (IA1 6.1)			OJL	ILT	
IA1 6.1	**Know:**	Practices and procedures for obtaining and installing **Public Key Infrastructure** (PKI) user certificates.			Ability to obtain and assist in installing and configuring PKI software certificates on a workstation or server.
	Do:	Successfully execute activities related to obtaining, installing and testing PKI certificates for end-user workstations and servers.	16		
	ILT:				
	Exit:	Execute activities for user account management and management of access privileges such as PKI.			
IA1 6.2	**Know:**	Basics of the organizational **anti-virus** practices and tools.			Ability to support and maintain organizational anti-virus services.
	Do:	Successfully install, configure and maintain anti-virus software on organizational servers. Successful and complete participation in operating and maintaining organizational virus perimeter systems and workstation anti-virus definition servers.	40		
	ILT:				
	Exit:	Successful installation, configuration and maintenance of organization's anti-virus services.			
IA1 6.3	**Know:**	Organization's practices and procedures for installing, configuring and maintaining **workstation and network firewalls.**			Ability to install and properly configure basic

	Do:	Successfully install, configure and maintain firewall services such as; workstation firewalls, subnet firewalls, organizational firewalls, etc. Participate in installing firewall block and exception lists. Participate in firewall log analysis and reporting of anomalies.	120		workstation and network firewalls.
	ILT:	Security Concepts		40	
	Exit:	Successfully conduct firewall installations, configurations and maintenance activities.			
IA1 6.4	**Know:**	Basic **concepts,** configurations and policies related to the organization's **firewall** services**.**			Ability to discuss and communicate basic information about the organization's firewall.
	Do:	Accurately describe the organization's firewall policies, configurations and general concepts. Deliver a short paper or presentation to a security audience demonstrating a working knowledge of the organization's firewall concepts, policies and practices.	80		
	ILT:				
	Exit:	A short paper or presentation to a security audience demonstrating a working knowledge of the organization's firewall concepts, policies and practices.			
IA1 6.5	**Know:**	Practices and procedures for monitoring network **Intrusion Detection Systems** (IDS).			Ability to monitor network IDS; to configure IDS alerts and to perform IDS log analysis and incident reporting.
	Do:	Accurately describe procedures for monitoring, assessing and reporting incidents detected by the organizations IDS. Participate in the establishment of IDS alerts, IDS log analysis and incident reporting practices. Conduct IDS monitoring, analysis and reporting activities.	80		
	ILT:				
	Exit:	Conduct IDS monitoring, analysis and reporting activities.			
IA1 6.6	**Know:**	How to analyze incoming packets and protect the network using tools as Snort, Ethernet, firewalls and route nulling.			Ability to manage Intrusion Detection systems.
	Do:	**Manage Intrusion Detection Systems** - understand incoming packets for potential hostile intent and take protective action if required.	120		
	ILT:				
	Exit:	Install and configure an IDS system and capture a packet based on implemented signatures.			
IA1 6.7	**Know:**	The difference between different types of firewalls and **firewall management concepts.**			Ability to manage the firewalls.

			Hours		Job Related Competencies
	Do:	Ability to analyze the requirements for a firewall entry, make the entry, and apply it to an interface. Understanding the difference between different types of firewalls.	80		
	ILT:				
	Exit:	Analyze the requirements for a firewall entry, explain conclusions, make the entry, and then apply it to an interface. Recover from errors.			
IA1 6.8	**Know:**	**Identification & Authentication Concepts.**			Ability to understand the various methods of identification and authentications concepts for windows environments.
	Do:	Become familiar with identification and authentication concepts for windows environments (local, domain, etc…).	80		
	ILT:				
	Exit:	Describe the various methods of identification and authentications concepts for windows environments.			
Information Assurance Specialization - Soft Skills (IA1 7.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA1 7.6	**Know:**	**ORAL COMMUNICATIONS**			Listens to others; makes clear and effective oral presentations to individuals and groups.
	Do:	Participate in site visits. Assist in developing EEO Special Observances. Represent supervisor at meetings/conferences. Give briefings/presentations. Participate in professional organizations. Serve as guest lecturer for community events. Perform volunteer work. Serve as member of Workforce Diversity Council..	24		
	ILT:	Effective Briefing Techniques; Interpersonal Communications; Executive Writing & Speaking; Communication & Conflict Mgmt Skills; How to Make Presentations with Confidence & Power; Public Speaking; Speech Writing; Analysis & Delivery Business & Professional Communication.		40	
	Exit:	Listens to others; makes clear and effective oral presentations to individuals and groups.			
IA1 7.7	**Know:**	**WRITTEN COMMUNICATIONS**			Communicates effectively in writing; reviews and critiques others' writing.
	Do:	Attend meetings/conferences as recorder. Author/revise activity directives. Edit others' writing. Review correspondence/reports. Draft routine correspondence. Prepare reports. Request others proofread your writing & provide feedback.	24		

	ILT:	Spelling; Grammar & Punctuation Skills; Contemporary Navy Writing; Report Writing; Editing & Proofreading Skills; English Grammar & Usage; Technical Writing; Editing Your Own Writing; Writing Effective Letters & Memos; Executive Writing & Speaking; Proofreading & Editing Skills; Programmed Punctuation; Writing Analytical Reports; Business Communications; Professional Writing.	25	
	Exit:	Communicates effectively in writing; reviews and critiques others' writing.		
IA1 7.8	**Know:**	**PROBLEM SOLVING**		Recognizes and defines problems; analyzes relevant information; encourages alternative solutions and plans to solve problems.
	Do:	Shadow a supervisor. Shadow an EEO Counselor. Serve on a working group. Participate in brainstorming sessions to consider multi-decision alternatives. Keep a record of problems that arise to identify recurrent ones. Collect or locate references that may help you with future problem solving. Survey others to pin-point problem areas. Have brainstorming session to identify possible solutions to a problem; determine most viable solution.	24	
	ILT:	Creative Problem Solving & Decision Making; Workplace Skills.		
	Exit:	Recognizes and defines problems; analyzes relevant information; encourages alternative solutions and plans to solve problems.		
IA1 7.9	**Know:**	**ORGANIZATIONAL AWARENESS**		Possesses knowledge of the mission and organization of NUWC Keyport; including understanding how the organization fits into the entire DoN; understands the roles and responsibilities of each Division detachment and of the major NAVSEA claimants; and how those roles and responsibilities support the DoN mission
	Do:	Familiarize yourself with goals and missions and how they support and interrelate with each other. Network with others at all levels of the organizational hierarchy. Review local activity organizational manuals, telephone books, lists of directives, and command history reports to get a 'big picture" of the organization as a whole & how the various functions relate to each other	24	
	ILT:	.		
	Exit:	Possesses knowledge of the mission and organization; including understanding how the organization fits into mission.		
IA1	**Know:**	**INTERPERSONAL/TEAM SKILLS**		Considers and

7.10	**Do:**	Seek feedback from peers about your interpersonal skills. Serve as member/chair of a working group. Serve as member on EEO Committee. Participate in a professional, or other volunteer community organization. Serve on a team to formulate a POA&M. Chair a panel.	24		responds appropriately to the needs, feelings, capabilities and interests of others; maintains self-control in difficult situations; provides feedback in a constructive manner.
	ILT:	Interpersonal Communication; How to Handle Difficult People; Conflict Management Skills; Team Building; Assertiveness Skills; Communication & Conflict Management Skills; Effective Listening & Memory Development; Understanding Human Behavior; Business Professions Seminar; Human Relations; Workplace Skills; Speaking & Interpersonal Communication.			
	Exit:	Considers and responds appropriately to the needs, feelings, capabilities and interests of others; maintains self-control in difficult situations; provides feedback in a constructive manner.			
IA1 7.11	**Know:**	**SELF-DIRECTION**			Realistically assesses own strengths, weaknesses, and impact on others; seeks feedback from others; works persistently towards a goal; demonstrates self-confidence; invests in self-development; manages own time effectively.
	Do:	Set improvement goals and establish measures to gauge level of improvement. Evaluate IDP progress quarterly. Volunteer for special assignments and/or teams. Read "The 7 Habits of Highly Effective People" (Stephen R. Covey). Write down your goals, monitor your progress, & adjust as necessary. Share your goals with your supervisor & ask for feedback on your progress. Identify a new set of skills that would be beneficial to you and learn them. Keep a daily 'to-do" list & prioritize frequently. Establish firm deadlines for projects, including intermediate deadlines. Participate in professional/community organizations as a means of strengthening specific job-related skills (e.g., project management, public speaking, financial management, etc.). Keep a journal with task notes, lessons learned, goals achieved, etc.	24		
	ILT:	Time Management; Managing Multiple Priorities; How to Management Multiple Projects & Meet Deadlines; Decision Making for Support Staff; How to De-junk Your Life; First Things First; Assertiveness Skills; Career Communications; Goal-Setting.			

	Exit:	Realistically assesses own strengths, weaknesses, and impact on others; seeks feedback from others; works persistently towards a goal; demonstrates self-confidence; invests in self-development; manages own time effectively.			
IA1 7.12	**Know:**	**QUALITY PRINCIPLES**			Understands and applies quality principles such as teamwork, quantitative decision making, and continuous process improvement to meet or exceed customer expectations.
	Do:	Read books or periodicals that address Total Quality Management or Leadership principles (e.g., Deming, Covey, etc.). Join a working group involved in measuring customer satisfaction. Serve as facilitator for a working group. Develop and implement a survey to measure customer satisfaction. Develop reporting & tracking systems for your projects.	24		
	ILT:	Methods for Managing Quality; Total Quality Management; How to Measure Customer Satisfaction; Various TQL training; How to Deliver Exceptional Customer Service; Managing the Customer Satisfaction Process; Quality Control.			
	Exit:	Understands and applies quality principles such as teamwork, quantitative decision making, and continuous process improvement to meet or exceed customer expectations.			
IA1 7.13	**Know:**	**CUSTOMER ORIENTATION**			Actively seeks customer input; ensures customer's needs are met; continuously seeks to improve the quality of services, products, and processes. Balances customer desires with task requirements to produce a quality product or process.
	Do:	Identify your internal and external customers, and what they want and expect. Develop a presentation on quality improvement and customer satisfaction. Keep a record of and analyze complaints, missed deadlines, overtime worked, lost business, etc., to determine where improvements should be made. Design a system for surveying customer satisfaction that can be adjusted around the changing needs of customers. Network with people in other departments/organizations to determine how they analyze customer satisfaction.	24		
	ILT:	Measuring Customer Satisfaction; Quality Control; How to Handle Difficult People; Customer Service; Managing the Customer Satisfaction Process; Customer Service Excellence; Dealing with the Public; Dealing with Angry Customers; How to Deliver Exceptional Customer Service.			

	Exit:	Actively seeks customer input; ensures customer's needs are met; continuously seeks to improve the quality of services, products, and processes. Balances customer desires with task requirements to produce a quality product or process.			
IA1 7.14	**Know:**	**FLEXIBILITY**			Adapts to change in the work environment; effectively copes with stress.
	Do:	Perform duties in absence of supervisor. Assume Lead responsibilities. Volunteer for special assignments and/or teams. Develop multiple contingency plans. Cross-train in related field. Serve on a decision-making committee to develop multiple contingency plans.	24		
	ILT:	How to Handle Difficult People; Managing Change; Thinking Outside the Boundaries; Crisis Communication, Stress Management; How to Manage Multiple Projects & Meet Deadlines; Thinking Outside the Lines; Managing Multiple Projects; Objectives & Deadlines; Time Management; Organizational Change & Development			
	Exit:	Adapts to change in the work environment; effectively copes with stress.			
IA1 7.15	**Know:**	**DECISIVENESS**			Takes action and risks when needed; makes difficult decisions when necessary.
	Do:	Set a target date for a decision & plan the decision process accordingly. For a complex decision, create a flow chart with several decision points. Discuss with supervisor. Volunteer for assignments with tight timelines that force decisiveness (e.g., site visits, IGs, etc.). Serve as officer in volunteer organization. Chair a panel. Serve on teams that have a specific focus. Assist in the formulation of a POA&M. Serve as a sports referee/umpire.	24		
	ILT:	Assertiveness Skills; Decisiveness & Empowerment Skills; Time Management; Creative Problem Solving.			
	Exit:	Takes action and risks when needed; makes difficult decisions when necessary.			
IA1	**Know:**	**TECHNICAL COMPETENCE**			Demonstrates

			OJL	ILT	
7.16	**Do:**	Perform duties in absence of supervisor. Shadow supervisor. Network with other people in your field. Cross-train in related field. Attend technical-specific conference(s).Keep list of relevant resources in job-related fields. Join/participate in technical job-related professional organization (e.g., American Society of Military Comptrollers, etc.).Read technical/trade articles and periodicals. Give subject matter briefs. Consult with others who have technical skills/knowledge that you lack	24		technical proficiency and an understanding of its impact in areas of responsibility.
	ILT:	Various Computer Courses, Technical Training in your field			
	Exit:	Demonstrates technical proficiency and an understanding of its impact in areas of responsibility.			
IA1 7.17	**Know:**	**DIVERSITY AWARENESS**			Respects and values the strengths and unique offerings of different groups/individuals.
	Do:	Assist in EEO Special Observances. Serve on EEO Committee. Shadow assignment in EEO. Seek assignments where you are exposed to cultural diversity. Develop a plan to capitalize on the diversity of your work unit by thinking of ways in which each individual's unique talents & preferences can be drawn into the work process. Discuss plan with supervisor. Obtain statistics on local workforce demographics and analyze. Sponsor an overseas student. Participate in a service organization such as Big Brothers/Big Sisters, Literacy Program, etc.	28		
	ILT:	Valuing Diversity; Communication Skills; Prevention of Sexual Harassment; EEO for Supervisors; Introduction to Sociology; Gender & Communication; Race & Ethnic Relations; Sociology of Gender; Race & Ethnic Relations; EEO -- It's Place in the Federal Government.			
	Exit:				

Total   2000   350

Information Assurance Apprentice Technician Level 2					
Information Assurance Specialization - General (IA2 1.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA2 1.1	**Know:**	**Introduction to Privacy Laws, Regulations, Copyright, Trademark, & Patent infringement.**			Ability to determine the trade-offs between security, privacy and operations and

			OJL	ILT	
	Do:	Review, research and discuss privacy laws, regulations, copyright, trademark & patent infringement with regard to the organization.	40		the organizational liability.
	ILT:	_			
	Exit:	Provide a discussion paper describing potential impacts on organizations with regard to this subject.			
IA2 1.2	**Know:**	Understand reporting requirements and procedures of **incident reporting** in the event of a successful attack against our systems.			Ability to understand reporting requirements and procedures of incident reporting.
	Do:	Complete an incident report for a simulated successful attack.	40		
	ILT:	Incident/Response & Handling		40	
	Exit:	Concise and accurate incident report for a simulated successful attack.			
IA2 1.3	**Know:**	Organizations **physical security requirements -** Tempest, Harden rooms & safes, physically securing wiring closets, cable paths.			Ability to maintain the organizations physical security.
	Do:	Research and design a secure computer room with cryptographic equipment, acceptable to the senior engineer.	40		
	ILT:	_			
	Exit:	Provide a paper design for a secure computer room with cryptographic equipment, acceptable to the senior engineer.			
IA2 1.4	**Know:**	Policies and procedures that involve documents labeled **Business Sensitive, Foreign Access, etc.**			Ability to determine what data falls into what classification and the access controls.
	Do:	In-box exercise demonstrating proper marking of appropriate document.	40		
	ILT:	_			
	Exit:	Successfully perform in-box exercise demonstrating proper marking of appropriate document.			
IA3 1.1	**Know:**	**Security Management Organizational Concepts.**			Ability to understand the planning, organization and roles of individuals involved in security, develop security policies and utilize tools used to identify threats, classify assets and rate vulnerabilities.
	Do:		80		
	ILT:	Security Management Practices		40	
	Exit:				
Information Assurance Specialization - Network (IA2 2.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA2	**Know:**	**Advanced network troubleshooting** techniques.			Ability to resolve network problems using software

			Hours OJL	ILT	Job Related Competencies
2.1	**Do:**	Using basic tools such as ping, trace and others to isolate and repair a network problem.	80		tools.
	ILT:	Networking IV		40	
	Exit:	Successfully resolve problems using software tools.			
IA2 2.2	**Know:**	Knowledge of Windows and UNIX ports & protocols in **network designs.**			Ability to understand various network designs.
	Do:	Describe differences between tactical and non-tactical networks, develop notional tactical network designs, and describe typical tactical operating environments.	80		
	ILT:				
	Exit:	Successfully document understanding of various network designs.			
IA2 2.3	**Know:**	Troubleshooting techniques for **network monitoring and administration.**			Ability to provide secure network administration and monitoring.
	Do:	Monitor the network using tools such as e-mon and HP open view. Basic network troubleshooting.	80		
	ILT:	Network Security, Communication & Authentication		40	
	Exit:	Resolve problems using software tools.			
IA2 2.4	**Know:**	The various LAN technologies, when they are used and how they are implemented to support a **secure LAN.**			Ability to implement various technologies to keep the LAN secure.
	Do:	Implement various technologies to keep the LAN secure.	80		
	ILT:	Network Attacks, Computer Crime & Hacking		40	
	Exit:	Provide secure LAN administration.			
IA2 2.5	**Know:**	The various WAN technologies, when they are used and how they are implemented to support a **secure WAN.**			Ability to implement various technologies to keep the WAN secure.
	Do:	Implement various technologies to keep the WAN secure.	40		
	ILT:				
	Exit:	Provide secure WAN administration.			
IA2 2.6	**Know:**	**Server Back Up & Recovery best practices.**			Ability to implement best practices.
	Do:	Review, learn and compile server Back up & recovery best practices.	80		
	ILT:				
	Exit:	Successfully implement Server Back Up & recovery Best Practices			

Information Assurance Specialization - Services (IA2 3.1)		**Hours**		**Job Related Competencies**
		OJL	**ILT**	

			OJL	ILT	
IA2 3.1	**Know:**	How to employ the services and processes to handle NT Security and authentication, resolving (translating) human-friendly names into IP addresses recognizable by computers with WINs - M**anaging Active Directory Users/Group/Organizational Units.**			Ability to manage Active Directory Users/Group/Organizational Units.
	Do:	Understand the services and creation of Organizational Unit complete with policies and security assigned by coach.	80		
	ILT:				
	Exit:	Successfully and independently manage the Active Directory Users/Group/Organizational Units.			
IA2 3.2	**Know:**	How to employ the services and processes to handle Internet Address lookups, Reverse lookups, Mail Records, IP and IP Masking, and Dynamic Host Configuration Protocol setup - **Managing DNS (Domain Name Services).**			Ability to Manage DNS (Domain Names Services)
	Do:	Understand the concepts and Successful creation of DNS Forward/Reverse lookups, proficiency with the NSLOOKUP utility, Successful.	80		
	ILT:				
	Exit:	Successfully and independently manage the DNS.			
IA2 3.3	**Know:**	Various technologies to provide **Security support for PED's.**			Ability to provide security for PED's.
	Do:	Configure and troubleshoot PDA, cell phones, etc. research, discuss and learn best practices.	80		
	ILT:				
	Exit:	Provide a discussion paper on significant PED security threat.			
Information Assurance Specialization - Operations and Applications (IA2 4.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA2 4.1	**Know:**	How to administer Window 2000 System administration tasks and Administer Internet Information Server (IIS). Understand the primary security risks related to this technology.			Ability to provide web server administration.
	Do:	Participate in **Web Server Security Administration** by demonstrating installation and security configuration of IIS on a server in the IT test bed.	80		
	ILT:				

			OJL	ILT	
	Exit:	Demonstrate installation and security configuration of IIS on a server in the IT test bed. The server must successfully withstand an intrusion attempt.			
IA2 4.2	**Know:**	**Desktop Back Up & Recovery best practices.**			Ability to implement best practices.
	Do:	Review, learn and compile desktop Back up & recovery best practices.	80		
	ILT:				
	Exit:	Successfully implement desktop Back Up & recovery Best Practices.			
IA2 4.3	**Know:**	Customer requirements and develop a **database backup & recovery strategy** to meet identified requirements - with emphasis on data base and application software.			Ability to provide database backup & recovery.
	Do:	Participate in the development of a backup strategy.	80		
	ILT:				
	Exit:	Successfully develop a backup strategy based on customer requirements and demonstrate a successful recovery within times identified in requirements.			
Information Assurance Specialization - Practices (IA2 5.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA2 5.1	**Know:**	Guild lines in **Information Assurance Auditing.**			Ability to use guidelines in Information Assurance auditing.
	Do:	Perform an ST&E using National Security Agency, NIST and Navy guidelines.	80		
	ILT:				
	Exit:	Successfully provide ST&E.			
IA2 5.2	**Know:**	Knowledge of the tools and processes required for performing & interpreting **automated vulnerability scans** of the network. Knowledge of Windows and UNIX ports & protocols.			Ability to perform & interpret vulnerability scans of the network.
	Do:	Perform & interpret vulnerability scans.	40		
	ILT:				
	Exit:	Successfully and independently perform & interpret three or more vulnerability scans.			
IA2 5.3	**Know:**	Understanding how to request an **external scan** by Navy agencies certified to do scanning.			Ability to conduct external scans.
	Do:	Conduct External Scans	40		
	ILT:				
	Exit:	Complete a simulated request by preparing the proper correspondence.			

			Hours		Job Related Competencies
IA2 5.4	**Know:**	**Information Assurance Accreditation.**			Ability to perform formal accreditation of networks and/or applications.
	Do:	Understand and apply the accreditation process. Interpret and apply vulnerability scan results to prepare formal system accreditation documentation.	40		
	ILT:				
	Exit:	Perform formal accreditation of networks and/or applications.			
IA2 5.5	**Know:**	**Vulnerability Test & Evaluation** guidelines.			Ability to perform security test & evaluations.
	Do:	Perform a security test & evaluation using National Security Agency, NIST, SANS and organizational guidelines.	40		
	ILT:	Information Assurance Methodology (IAM) Training		40	
	Exit:	Perform security test & evaluations.			
IA2 5.6	**Know:**	**Information Assurance Accreditation Requirements**			Ability to assist with a formal DITSCAP accreditation of networks and/or applications.
	Do:	Understand of the requirements related to various aspects of the certification.	40		
	ILT:				
	Exit:	Assist with a formal DITSCAP accreditation of networks and/or applications.			
IA2 5.1	**Know:**	Understand quantitative and qualitative **risk analysis** methods, and the concept of residual risk.	24		Ability to provide risk/threat analysis.
	Do:	Risk/Threat Analysis			
	ILT:	Security Assessment		40	
	Exit:	Perform a Risk Assessment in conjunction with Business Case Analysis. Presenting findings in a briefing paper/group presentation.			

Information Assurance Specialization - Tools (IA2 6.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA2 6.1	**Know:**	The difference between different types of firewalls and **firewall management concepts.**			Ability to manage the firewalls.
	Do:	Ability to analyze the requirements for a firewall entry, make the entry, and apply it to an interface. Understanding the difference between different types of firewalls.	80		
	ILT:	Internet Firewalls and E-Commerce		40	
	Exit:	Analyze the requirements for a firewall entry, explain conclusions, make the entry, and then apply it to an interface. Recover from errors.			

			Hours		Job Related Competencies
IA2 6.2	**Know:**	Components to **Key System Administration (PKI).**			Ability to operate and maintain a Key Local Registration Authority Workstation.
	Do:	Install and configure a DoD Key Local Registration Authority Workstation.	80		
	ILT:				
	Exit:	Successfully and independently install and configure a Key Local Registration Authority Workstation.			
IA2 6.3	**Know:**	**Cryptography Concepts and Technology.**			Ability to apply cryptography concepts.
	Do:	Understand the military and commercial methods and applications of cryptography.	80		
	ILT:				
	Exit:	Describe differences and identify products for military and commercial applications.			
Information Assurance Specialization - Soft Skills (IA2 6.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA2 6.1	**Know:**	**SITUATIONAL LEADERSHIP**			Demonstrates and encourages high standards of behavior; adapts leadership style to situations and people; empowers, motivates and guides others.
	Do:	Seek out role models who exhibit good leadership practices and interview or shadow. Read books and listen to tapes on effective leadership and various leadership styles (e.g., Deming, Covey, etc.).Read books about successful managers (e.g., Lee Iacocca, Dave Thomas, Sam Walton, etc.). Review results of 360 Assessment to develop an understanding of your leadership style. Seek temporary assignment in your organization that provides increasing responsibilities to be accountable for a task or decision. Analyze your leadership style in relation to each of your employees (using instrument such as Myers-Briggs Inventory) and try to modify your behavior to most effectively capitalize on each employee's profile. Serve as an officer in a service organization. Serve as a project leader for a community exhibit/event. Serve as a spokesperson for an issue at a community meeting.	40		

	ILT:	Situational Approaches to Leadership; How to Supervise People; Introduction to Supervision; Supervision and Group Performance; Assertiveness Skills for Managers & Supervisors; Management Development Seminar ; 1001 Ways to Energize Employees; Critical Thinking; Working with Difficult People; Principles of Management; Fundamentals of Leadership; Organizational Behavior; Leadership; Effective Work Delegation; Criticism & Discipline Skills for Managers.			
	Exit:	Demonstrates and encourages high standards of behavior; adapts leadership style to situations and people; empowers, motivates and guides others.			
IA2 6.2	**Know:**	**DEMONSTRATE CORE VALUES**			Exhibits through personal performance the principles of honor (ethical behavior), commitment (technical excellence and quality of work), and courage (mental strength to do what is right).
	Do:	Review Code of Ethics (Public Law 96-303 & 5 CFR Part 2635) periodically. Flow chart your job, re-evaluate annually, and apply improvements. Maintain a professional demeanor in interaction with others. Volunteer in community organizations in which you serve as role model (e.g., Big Brothers/Big Sisters, Literacy Program, etc.).Continuously update your knowledge of policies and regulations that apply to your area.	24		
	ILT:	Ethics; Ethics in Business			
	Exit:	Exhibits through personal performance the principles of honor (ethical behavior), commitment (technical excellence and quality of work), and courage (mental strength to do what is right).			
IA2 6.3	**Know:**	**MANAGING DIVERSE WORKFORCE**			Recognizes the value of culture, ethnic, gender, and other individual differences; provides employment and development opportunities for a diverse workforce.
	Do:	Familiarize yourself with EEO & Affirmative Action rules and policies. Familiarize yourself with discrimination complaints process. Serve on an EEO Committee. Serve on an activity Awards Committee. Help organize a Special Emphasis event. Evaluate the developmental needs of the employees in your work group.	40		

	ILT:	Managing Workforce Diversity; How to Become a Great Communicator; Multicultural Workforce Management; EEO for Supervisors; Prevention of Sexual Harassment; Introduction to Sociology; Gender & Communication; Psychology of Work Force Diversity; Intercultural Communications; Race & Ethnic Relations; Sociology of Gender			
	Exit:	Recognizes the value of culture, ethnic, gender, and other individual differences; provides employment and development opportunities for a diverse workforce.			
IA2 6.4	**Know:**	**COACHING/COUNSELING**			Develops skills in observation, listening, and one-on-one teaching; applies them to assist others to learn and continually improve their performance; and provides effective feedback; develops the ability to counsel others to help them to achieve personal and professional growth.
	Do:	Develop coaching/counseling skills through involvement in a service organization (e.g., Scouting, team sports, Big Brother/Big Sisters, etc.).Read books on coaching/counseling skills. Ask employees to identify the areas in which they would find one-on-one teaching to be the most helpful; develop a plan for providing identified training. Shadow a senior manager. Perform duties in absence of supervisor.	32		
	ILT:	Effective Listening Skills; Coaching and Teambuilding Skills for Supervisors & Managers; How to Give Constructive Feedback; Coaching Skills for Managers & Super-visors; Coaching to Increase Productivity ; Coaching, Criticism & Discipline Skills for Managers & Supervisors; Introduction to Psychology; Applied Psychology; Introduction to Sociology; Human Relations; The Helping Relationship; Introduction to Behavior Modification; Business & Industrial Psychology.			
	Exit:	Develops skills in observation, listening, and one-on-one teaching; applies them to assist others to learn and continually improve their performance; and provides effective feedback; develops the ability to counsel others to help them to achieve personal and professional growth.			
IA2	**Know:**	**CONFLICT MANAGEMENT**			Anticipates and seeks to

6.5	**Do:**	Discuss with your supervisor a situation in which you had to exhibit conflict management skills and ask for feedback on how you handled it. Practice active listening skills. Serve on a liaison/mediator working group to resolve organizational problems/issues. Perform duties in absence of supervisor. Observe Labor Relations contract negotiation meetings.	40			resolve confrontations, disagreements, and complaints in a constructive manner.
	ILT:	How to Handle Difficult People; Conflict Management Skills; Conflict Management & Confrontational Skills ; Responding to Conflict; How to Handle People with Tact & Skill; Positive Approaches to Difficult People.				
	Exit:	Anticipates and seeks to resolve confrontations, disagreements, and complaints in a constructive manner.				
IA2 6.6	**Know:**	**CHANGE MANAGEMENT**				Serves as a positive agent for change in the organization's structural alignment, climate, or operational processes. Learns about and proactively advocates and influences adoption of promising new ideas, methods, services, and products from knowledge of best practices in government and industry.
	Do:	Keep up-to-date by reading emerging political, economic and technological changes. Meet with a manager who has successfully implemented a change; discuss the steps he/she took throughout the change process; review your own plans for change with this person and ask for feedback. Assist others in gathering information. Implement a change in your work unit by identifying a problem situation that needs changing, deciding what changes are needed, developing & choosing alternatives and then making the necessary change. Volunteer to serve on working group established to survey the need for change and/or determine change policies & procedures. Read books/articles on change management, such as: Organization Development & Change, (Huse &Cummings), or Checklist for Change, (Harvey). Serve on a working group to develop organizational vision statements and long range plans.				
	ILT:	Change Management; Models for Change; Various TQL Courses; Leadership: Change, Challenge & Empowerment; Organizational Change & Development; Managing Organizational Change				

	Exit:	Serves as a positive agent for change in the organization's structural alignment, climate, or operational processes. Learns about and proactively advocates and influences adoption of promising new ideas, methods, services, and products from knowledge of best practices in government and industry.			
IA2 6.7	**Know:**	**TEAM BUILDING**			Considers and responds appropriately to the needs, feelings, capabilities and interests of others; provides feedback; treats others equitably; fosters cooperation, communication, and consensus among groups.
	Do:	Serve on a project team. Hold brainstorming sessions. Serve as an officer in a professional/community organization. Chair a panel .Participate in community organizations (e.g., Scouting, sports, religious groups, etc.)Perform duties in absence of supervisor.	40		
	ILT:	How to Lead a Team; Fundamentals of Team Building; Performance Management of a Team; Meeting Skills for Super-visors & Managers; Jump-Starting High-Performing Teams; How to be a More Effective Team Leader; Team Building; Sociology of Small Groups; Team Building & Team Leadership; Effective Work Delegation; Delegation & Empowerment; Project Management Skills for Teams.			
	Exit:	Considers and responds appropriately to the needs, feelings, capabilities and interests of others; provides feedback; treats others equitably; fosters cooperation, communication, and consensus among groups.			
IA2 6.8	**Know:**	**INFLUENCING/NEGOTIATING**			Networks with and provides information to key groups and individuals; appropriately uses negotiation, persuasion and authority in dealing with others to achieve goals.
	Do:	Volunteer for assignments that require interaction with members of different activities and levels. Participate in a community organization (e.g., Scouting, YMCA, church, Navy Kids, etc.)Read books on influencing people, such as *How to Make Friends & influence People,* (Dale Carnegie).Serve as a liaison/POC for an organizational objective. Observe Labor Relations contract negotiation meetings. Shadow a senior manager. Perform duties in absence of supervisor. Volunteer for site visits. Serve as a spokesperson for an issue at a community meeting.	40		

			OJL	ILT	
	ILT:	Assertiveness Skills; Negotiation Skills; Active Listening; Delegation & Empowerment; Alternative Dispute Resolution; 1001 Ways to Energize Employees; Introduction to Sociology; Persuasive Communication.			
	Exit:	Networks with and provides information to key groups and individuals; appropriately uses negotiation, persuasion and authority in dealing with others to achieve goals.			
IA2 6.9	**Know:**	**HUMAN RESOURCES MANAGEMENT**			Ensures effective recruitment, selection, training, performance appraisal, recognition and corrective/disciplinary action; promotes affirmative employment, good labor relations, and employee well-being.
	Do:	Define & write/revise a job description for a position in your department. Familiarize yourself with Federal hiring rules & regulations. Read EEO & Affirmative Action guidelines. Establish & implement developmental assignments for new & seasoned employees in your work unit to enhance their performance and maturity on the job. Review the current performance appraisal elements/standards of your employees, analyze their measurability & appropriateness to their jobs, & make changes as necessary. (Seek assistance from the personnel office, as needed.)Familiarize yourself with procedures to reward and discipline employee performance. Familiarize yourself with employment policies. Familiarize yourself with grievance procedures.	40		
	ILT:	Management & Organizational Behavior; Personnel Management; Industrial-organizational Psychology		30	
	Exit:	Ensures effective recruitment, selection, training, performance appraisal, recognition and corrective/disciplinary action; promotes affirmative employment, good labor relations, and employee well-being			
			2000	**350**	

Information Assurance Apprentice Technician Level 3			
Information Assurance Specialization - General (IA3 1.1)	**Hours**		**Job Related Competencies**
	OJL	**ILT**	

			Hours		Job Related Competencies
IA3 1.1	**Know:**	**Introduction to Best Industrial Practice (DoD only - DoD/Comsec).**			Ability to implement best industrial security practice.
	Do:	Understand the equipment and processes employed to protect transmissions of classified data.	40		
	ILT:				
	Exit:	Explain the purpose, high-level architecture, and major components of the (DoD Electronic Key Management System).			
IA3 1.2	**Know:**	**Operations Security Policy.**			Ability to incorporate sucessful operational security practices, procedures and policies in the organization.
	Do:	Study local and higher level practices, procedures and policies relating to operations security.	40		
	ILT:				
	Exit:	Explain how operational security supports an organization.			
IA3 1.3	**Know:**	**Security Management Employment Polices & Practices.**			Ability to incorporate sucessful security management employment policies in the organization.
	Do:	Study local and higher level directives relating to personnel security.	80		
	ILT:				
	Exit:	Explain how personnel security relates to new hires and current employees.			
IA3 1.4	**Know:**	**Security Awareness & Training.**			Ability to develop and implement security awareness training in the organization.
	Do:	Research user security policies, procedures, and training requirements for the organization.	40		
	ILT:	Design and Development of Instruction Materials and resources		40	
	Exit:	Develop a user awareness briefing.			
IA3 1.5	**Know:**	**Advanced Concepts (Law, Investigations & Ethics).**			Ability to understand federal and state law with regard to cyber crime.
	Do:	Study federal and state law with regard to cyber crime.	40		
	ILT:	Cyber law		40	
	Exit:	Provide a discussion paper describing or citing specific law governing cyber crimes.			

Information Assurance Specialization - Network (IA3 2.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA3 2.1	**Know:**	**Advanced Network Security Design** (firewalls, IDS) concepts and practices.			Ability to set up and design networks using good industry design practices.
	Do:	Set up and design networks using good industry design practices - using various network devices.	80		

			OJL	ILT	
	ILT:			40	
	Exit:	Successfully and independently set up and design a secure network.			
IA3 2.2	**Know:**	When to use various **remote services** and how to properly configure the services.			Ability to configure and secure remote services.
	Do:	Build, configure and assess (security scans) on RAS,VPN and OWA.	80		
	ILT:				
	Exit:	Successfully and independently configure and secure Remote Services.			
IA3 2.3	**Know:**	Concepts of **Network Attack Scenarios.**			Ability to understand the concepts, attack types and various security risks associated with network attacks.
	Do:	Understand the concepts, attack types and various security risks associated with network attacks.	40		
	ILT:	_		40	
	Exit:	Successfully attacking a honeypot system in an Information Warfare lab environment, or providing a paper or presentation on this subject to a team or at a information sharing forum.			
IA3 2.4	**Know:**	**Wireless Networking Security- Emanation Security Requirements.**			Ability to incorporate wireless networking in to the organization with security considerations.
	Do:	Use tools such as WEPcrack and Snort to explore and assess Wi-Fi vulnerabilities.	80		
	ILT:	DB, NW, Web and Wireless Security Issues and Strategies.			
	Exit:	Provide a discussion paper on the vulnerabilities, latest developments, and mitigation actions for securing wireless IEEE 802.11 (Wi-Fi) equipment.			
IA3 2.5	**Know:**	**Advanced Tactical Network Security Design.**			Ability to set up and design tactical networks.
	Do:	Setting up and designing tactical networks.	80		
	ILT:	Studies in Network Security		40	
	Exit:	Develop a drawing of a mock tactical network connecting several locations.			

Information Assurance Specialization - EMail Services (IA3 3.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA3 3.1	**Know:**	Understanding the **servers, processes** and privacy employed to transmit **e-mail.**			Ability to secure E-Mail Services.
	Do:	Build, configure and assess (security scan) an email service.	80		
	ILT:				
	Exit:	Successfully and independently build, configure and assess (security scan) an email service.			

IA3 3.2	**Know:**	**Multi-Media Security** concepts.			Ability to provide Multi-media security.
	Do:	Understand the basic vulnerabilities of multi-media collaboration tools on the desktop.	40		
	ILT:				
	Exit:	Provide a discussion paper on a significant security threat to a specific desktop collaboration tool such as Netmeeting or Messenger.			
IA3 3.3	**Know:**	**Messaging Systems -** concepts and equipment. (DOD only)			Ability to understand and explain military messaging systems.
	Do:	Understand the equipment and processes employed to digitally sign, encrypt and transmit, receive and distribute military organizational messages.	40		
	ILT:				
	Exit:	Explaining the purpose, high-level architecture, and major components of the DoD Defense Message System.			
IA3 3.4	**Know:**	**Desktop Forensic Analysis** concepts.			Ability to assist in desktop forensic analysis.
	Do:	Assist in examining, protecting and interpreting the evidence of attempted and successful computer intrusions.	80		
	ILT:			40	
	Exit:	Understanding the legal and technical aspects of protecting and interpreting intrusion evidence from audit trails and logs.			
IA3 3.5	**Know:**	The vulnerabilities and security configuration options of collaborative server tools.			Ability to provide securing collaborative work environments.
	Do:	Research , learn and discuss threats to **collaborative work environments**.	80		
	ILT:				
	Exit:	Provide a discussion paper on a significant security threat to a specific server collaboration tool such as Microsoft Sharepoint Portal.			
IA3 3.6	**Know:**	Customer requirements and develop a backup strategy to meet identified requirements - with emphasis on data base and application software.			Ability to provide advanced desktop back up and recovery.
	Do:	**Advanced Desktop Back Up & recovery.**	80		
	ILT:				

			OJL	ILT	
	Exit:	Successfully develop a backup strategy based on customer requirements and demonstrate a successful recovery within times identified in requirements.			
Information Assurance Specialization - Operations and Applications (IA3 4.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA3 4.1	**Know:**	Visual Studio .NET, ASP and the development of Web interfaces.			Ability to deploy a simple web application and a successful security scan.
	Do:	Develop and deploy a simple **web application** with a successful security scan.	80		
	ILT:				
	Exit:	Successfully and independently develop and deploy a simple web application with a successful security scan.			
IA3 4.2	**Know:**	**SQL Data Base Design with Security Emphasis.**			Ability to provide SQL Data Base Design with Security Emphasis.
	Do:	Research customer requirements and develop a backup strategy to meet identified requirements - with emphasis on data base and application software.	80		
	ILT:				
	Exit:	Successfully develop an ERD for an application which is validated by a Senior Developer for proper construction/elements.			
IA3 4.3	**Know:**	**SQL Server Security Administration.**			Ability to provide SQL Server Security Administration.
	Do:	Research, learn and discuss skills required to administer SQL server. Understand the primary security risks related to this technology.	40		
	ILT:				
	Exit:	Successfully and independently install and securely configure a SQL Server on a server in the IT test bed. The server must successfully withstand an intrusion attempt.			
IA3 4.4	**Know:**	**Advanced Data Base Back Up & recovery.**			Ability to provide data base back up & recovery.
	Do:	Determine customer requirements and develop a backup strategy to meet identified requirements - with emphasis on data base and application software.	40		
	ILT:				
	Exit:	Successfully develop a backup strategy and demonstrate a successful recovery within times identified in requirements.			

			OJL	ILT	
IA3 4.5	**Know:**	Knowledge of the processes and configurations employed to provide disaster recovery services.			Ability to provide disaster recovery services.
	Do:	**Advanced Server Back Up & recovery.**	40		
	ILT:				
	Exit:	Recovering an Exchange Server in the lab and an Individual e-mail message in production.			
Information Assurance Specialization - Practices (IA3 5.1)			**Hours**		**Job Related Competencies**
			OJL	**ILT**	
IA3 5.1	**Know:**	The proper procedures showing due care and reporting compliance with Information Assurance actions.			Ability to perform vulnerability alert actions.
	Do:	Assist in **Information Assurance Vulnerability Alert Actions.**	40		
	ILT:				
	Exit:	Assist the Information System Security Manager in processing the response to an IAVA security update action.			
IA3 5.2	**Know:**	The policies, rules and regulations related to proper use of **auditing user services**. Understand the tools used to monitor and prevent inappropriate use. Understand actions to be taken when inappropriate use is detected.			Ability to audit user services.
	Do:	Assist in auditing User Services.	40		
	ILT:	Auditing		40	
	Exit:	Successfully Configuring Internet blocks and monitoring email traffic using authorized tools and authorized test accounts in the production environment. Reviewing monitor logs and identifying trends and anomalies.			
IA3 5.3	**Know:**	Advanced concepts in IA **forensic analysis**.			Ability to support forensic analysis.
	Do:	Understand the legal and technical aspects of protecting and interpreting intrusion evidence from audit trails and logs.	80		
	ILT:	Forensics		40	
	Exit:	Explain the process of examining, protecting and interpreting the evidence of attempted and successful computer intrusions.			
IA3 5.4	**Know:**	**Security Monitoring, Traffic and Trend Analysis** concepts.			Ability to provide security monitoring, traffic and trend analysis.
	Do:	Assist in security monitoring, traffic and trend analysis.	80		
	ILT:				

			OJL	ILT	
	Exit:	Successfully identify patterns associated with various malicious attacks (DoS, Spoofing, etc…).			
IA3 5.5	**Know:**	**System Accreditation & Information Assurance Certification Requirements**			Ability to perform formal accreditation of networks and/or applications.
	Do:	Understand and apply the DITSCAP accreditation process. Interpret and apply ST& E and vulnerability scan results to prepare formal system accreditation documentation.	40		
	ILT:				
	Exit:	Perform three or more formal DITSCAP accreditations of networks and/or applications. (NX 4015)			

Information Assurance Specialization - Tools (IA3 6.1)			Hours		Job Related Competencies
			OJL	ILT	
IA3 6.1	**Know:**	**Advanced Identification & Authentication Concepts**			Ability to configure an environment using advanced identification and authentication concepts (PKI, Common Access Card, biometrics, etc…).
	Do:	Research the use of advanced identification and authentication concepts (PKI, Common Access Card, biometrics, etc…).	80		
	ILT:	_			
	Exit:	Configure an environment using advanced identification and authentication concepts (PKI, Common Access Card, biometrics, etc…).			
IA3 6.2	**Know:**	**Advanced Access Controls Concepts.**			
	Do:		80		
	ILT:				
	Exit:				
IA3 6.3	**Know:**	**Advanced Cryptography Concepts & Technology.**			Ability to use encryption techniques for secure data.
	Do:	Understand the techniques, strengths and weaknesses of selected encryption systems (military).	80		
	ILT:	Cryptography		30	
	Exit:	Correctly select, install and configure a cryptographically protected information system using Type 1 encryption techniques to protect Secret data. (military)			

Information Assurance Specialization - Soft Skills (IA3 8.1)			Hours		Job Related Competencies
			OJL	ILT	
IA3 8.1	**Know:**	**INNOVATIVE THINKING**			Develops insights and solutions; fosters

	Do:	Hold a brainstorming session with your work unit to discuss a current situation/problem, encourage creative ideas, record every idea, and then evaluate options. Make a list of several problems you face, rewrite each problem as an objective, list several creative ways to reach each objective, and discuss the findings with your supervisor Participate in professional organizations and stay current in the professional literature to keep track of the newest developments in your field. Formulate a POA&M for a major tasking. Read and write book reports on visionaries (e.g., Stephen R Covey, Avraham Y. Goldratt, Joel Barker, etc.).Serve on a team established to solve a specific problem.	20		innovation among others.
	ILT:	Creative Problem Solving ; Thinking Outside the Lines; Benchmarking: The Tool to Improve Competitiveness; Oral Communications; Customer Service; Thinking Outside the Boundaries; Creative Thinking; 1001 Ways to Energize Employees.			
	Exit:	Develops insights and solutions; fosters innovation among others			
IA3 8.2	**Know:**	**PROGRAM DEVELOPMENT PLANNING & EVALUATION**	20		Establishes policies, guidelines, plans, and priorities; identifies required resources; plans and coordinates with others; monitors progress and evaluates outcomes; improves organizational efficiency and effectiveness.
	Do:	Formulate an operational plan. Develop an annual set of goals for your work unit, specify interim goals and due dates, and evaluate monthly to check accomplishments. For each unit goal, develop a detailed plan of accomplishment. Serve on a strategic planning task force. Develop project management tracking system. Create a bulletin board to list goals/objectives & progress to-date. Serve on a cross-functional project team. Develop a POA&M. Formulate lessons learned on a specific project/program into a report.			
	ILT:	Project Management; Management Problems of the Technical Person in a Leadership Role; Program Planning & Analysis; Advanced Management Analysis; Performance Measurement: Financial & Program Evaluation; Fundamentals of Successful Project Management; Strategic Planning; Performance Measurements for Your Business; Statistical Process Control; Introduction to Management Science; Operations Management; Policy Analysis & Formulation.			

	Exit:	Establishes policies, guidelines, plans, and priorities; identifies required resources; plans and coordinates with others; monitors progress and evaluates outcomes; improves organizational efficiency and effectiveness			
IA3 8.3	**Know:**	**MODEL/REINFORCE CORE VALUES**			Exhibits through personal performance and example the principles of honor (ethical behavior), commitment (technical excellence and quality of work), and courage (mental strength to do what is right).
	Do:	Review Code of Ethics (Public Law 96-303 & 5 CYR Part 2635) periodically. Discuss with supervisor situations in which you demonstrated strong values and ethics. Ask for suggestions as to how you can demonstrate those values more effectively in future situations. Give briefs on Ethics to work group. Read and report to supervisor on books such as *The 7 Habits of Highly Effective People,* (Stephen R.Covey), Managing Organizational Behavior, (John R. Schennerhom), The Power of Ethical Management, (Kenneth Blanchard & Norman Vincent Peale), Principle-Centered Leadership, (Stephen R. Covey), or Making Ethical Decisions, (Michael Josephson).	16		
	ILT:	Ethics; Ethics in Business.			
	Exit:	Exhibits through personal performance and example the principles of honor (ethical behavior), commitment (technical excellence and quality of work), and courage (mental strength to do what is right).			
IA3 8.4	**Know:**	**RESOURCE MANAGEMENT**			Prepares and justifies budget; monitors expenses; manages procurement and contracting.
	Do:	Familiarize yourself with Keyport's financial position. Develop a budget plan for a specific project. Identify & request the resources required to reach an objective. Attend open budget hearings. Shadow your organization's Budget and/or Contract Officer, or serve a temporary assignment in the Budget/Finance &/or Contract Office. Ask others in your organization how they monitor expenses & budgets. Review agency & Federal Government procurement guidelines. Participate in a POM process.	20		

	ILT:	Budget justification & Presentation; Federal Budgetary Policy & Processes; Introduction to Managerial Accounting; How to Develop & Administer a Budget; Controlling a Unit Budget; Developing a Budget for a Unit; Federal Budget Process; Budget Execution; Budget Formulation; Federal Appropriation Law; Defense Resources Management Course; Introduction to Federal Acquisition; Contracting Basics for Support & Administrative Personnel; Managing Government Contracts; Governmental/Not-for-Profit Accounting; Applied Managerial Accounting; Managerial Finance.			
	Exit:	Prepares and justifies budget; monitors expenses; manages procurement and contracting.			
IA3 8.5	**Know:**	**TECHNOLOGY MANAGEMENT**			Encourages staff to stay informed about new technology; applies new technologies to organizational needs; ensures staff is trained and capable.
	Do:	Attend state-of-the-art trade shows. Read technical magazines & journals. Compile a list of resources in technical subject areas. Network with others in your field. Participate in professional technical organizations. Stay current in the professional literature to keep track of the newest developments in your field. Serve on a team to plan for the introduction of & training for a new technology.	20		
	ILT:	Management of Information Technology; Science, Technology & Public Policy; Information Systems Project Management; Special Topics in Business Data Processing; Computer Technology; Computers & Society; Management Information Systems.			
	Exit:	Encourages staff to stay informed about new technology; applies new technologies to organizational needs; ensures staff is trained and capable.			
IA3 8.6	**Know:**	**PROCESS OVERSIGHT MANAGEMENT**			Develops/demonstrates the ability to examine systems

	Do:	Develop a process flowchart for a major activity within your area of responsibility; identify & evaluate major control points.Use total quality tools (such as workflow documentation, root-cause analysis, etc.) to uncover opportunities for improvement in a work process.Read related books, such as: Organization Development & Change, (Huse), Out of the Crisis, (Deming), or Deming's Road to Continual Improvement, (Scherkenback).Interview Program Managers for insight into the oversight of their programs.	20		and work flows within the organization to facilitate process assessment and improvement.
	ILT:	Project Management; Introduction to Management Analysis; Intermediate Management Analysis; Advanced Management Analysis; Reengineering in the Public Sector; Business Process Reengineering; TQL Training; Quality Control Statistics; Total Quality Management; Quality Control; Basic Statistics; Introduction to Operations Research; Customer Service Excellence; Managing the Customer Satisfaction Process.			
	Exit:	Develops/demonstrates the ability to examine systems and work flows within the organization to facilitate process assessment and improvement.			
IA3 8.7	**Know:**	**MENTORING**			Develops the ability to counsel others to help them to achieve personal and professional growth.
	Do:	Participate in community mentoring/tutoring programs (e.g., Big Brothers/Big Sisters, Literacy Program, etc.).Discuss mentoring skills with a peer/manager who has proven to be successful.	20		
	ILT:	Mentoring Skills; Mentoring for Outstanding job Performance; Coaching Skills; Motivation Techniques; How to Give Constructive Feedback; Coaching Skills for Managers & Supervisors; Coaching to Increase Productivity; The Helping Relationship; Introduction to Behavior Modification..			
	Exit:	Develops the ability to counsel others to help them to achieve personal and professional growth.			
IA3 8.8	**Know:**	**PRESENTATION/MARKETING SKILLS**			Demonstrates the ability to clearly articulate, present,

	Do:	Develop standard promotional materials, presentations or statements. Represent your activity at meetings/conferences. Promote personal accomplishments. Seek opportunities to represent your organization, its goals & accomplishments in informal or formal gatherings. Develop & present a briefing or seminar. Participate in Toastmasters or other public speaking organizations. Shadow a senior manager. Perform duties in absence of supervisor.	16		and promote ideas and issues before a wide range of audiences, including senior officials, in such a manner as to ensure program credibility.
	ILT:	Public Speaking; Effective Briefing Techniques; Speech Writing; Analysis & Delivery; Marketing; Executive Communications Workshop; Strategies for Developing Effective Presentation Skills; Persuasive Communication; Business & Professional Communication; How to Make Presentations with Confidence & Power.			
	Exit:	Demonstrates the ability to clearly articulate, present, and promote ideas and issues before a wide range of audiences, including senior officials, in such a manner as to ensure program credibility.			
IA3 8.9	**Know:**	**RISK MANAGEMENT**			Identifies potential risks to product/program/processes early and implements effective abatement or control measures; defines evaluation criteria early and continuously collects, assesses, shares and responds to data appropriately.
	Do:	Examine successful projects to identify factors accounting for success. Develop a work unit performance standard with your employees; identify critical milestones for process review. Participate in strategic planning groups.	16		
	ILT:	Risk Management for Project Mangers; Introduction to Risk Management; Risk Analysis & Management.			
	Exit:	Identifies potential risks to product/program/processes early and implements effective abatement or control measures; defines evaluation criteria early and continuously collects, assesses, shares and responds to data appropriately.			
IA3 8.11	**Know:**	**STRATEGIC VISION**			Creates a shared vision of the organization; promotes

	Do:	Create a vision of where you'd like to see your department/organization in five years, evaluate alternative routes, and decide on a specific course to reach the chosen destination. Participate in a long-range planning session with other managers. Attend management meetings. Volunteer to help a community organization formulate a vision & strategic plan. Read books on strategic vision, such as: *Rethinking the Organization/The Architecture of Change,* (Tomasko), *A Force for Change,* (Kotter), *Competing for the Future,* (Hamel & Prahalad), and *Built to Last: Successful Habits of Visionary Companies*, (Collins & Porras).Attend strategic planning meetings as a participant, or observer. Interview a senior-level manager with strategic planning responsibilities.	8		wide ownership; champions organizational change
	ILT:	Executive Development Seminar; Strategies for Building High Performing Organizations; Strategic Planning: GPRA & NTR-Based; Strategic Planning; Tools & Techniques for Thinking & Managing Strategically; Strategy implementation; Transitioning to a Team-Based Environment.			
	Exit:	Creates a shared vision of the organization; promotes wide ownership; champions organizational change			
IA3 8.12	**Know:**	**EXTERNAL AWARENESS**			Stays informed on laws, policies, politics, Administration priorities, trends, special interests, and other issues; considers external impact of statements and actions; uses information in decision making.
	Do:	Survey external customer satisfaction. Attend inter-organizational meetings & seminars. Join and actively participate in professional organizations. Read articles and journals in your area of expertise and in other areas for which you are not directly responsible .Stay abreast of Federal policies by reading Congressional newsletters, the Federal Times, Federal Employees News Digest, and other sources of Federal updates. Read newspaper and journal articles to stay up-to-date on political & social trends. Attend DON programs/symposiums	8		

	ILT:	Developing Customer Focused Organizations; Dynamics of Public Policy; Capitol Hill Workshop; American National Government; Business, Ethics & Society; Public Administration Professional; Issues in American Government and Politics; Principles of Macroeconomics; American National Government; Executive Development Seminar; Executive Forum on Current Issues.			
	Exit:	Stays informed on laws, policies, politics, Administration priorities, trends, special interests, and other issues; considers external impact of statements and actions; uses information in decision making.			
IA3 8.13	**Know:**	**ORGANIZATIONAL REPRESENTATION & LIAISON**			Establishes and maintains relationships with key individuals/groups outside immediate work unit and serves as spokesperson for the organization.
	Do:	Join and become active in professional organizations & seek roles that provide visibility. Network with people outside of your organization who hold positions similar to yours. Volunteer to serve on a task force that deals with a problem relevant to your organization's future. Volunteer for assignments that require interaction with members of different organizational units & levels. Publicize activities and accomplishments of your organization (through bulletin boards, activity newsletter, Intranet, etc.).	16		
	ILT:	Executive Communications Workshop; Effective Executive Speaking; Advanced Executive Speaking; Public Relations: Strategies for Success; Organizational Communication; Promotional Management; Principles of Public Relations.			
	Exit:	Establishes and maintains relationships with key individuals/groups outside immediate work unit and serves as spokesperson for the organization.			
		TOTAL OJT HOURS and CLASSROOM	**2000**	**350**	

RELATED INSTRUCTION SCHEDULE FOR:
INFORMATION ASSURANCE

METHOD OF DELIVERY: *IN HOUSE TRAINING, COMMUNITY COLLEGE, UNIVERSITY, PRIVATE INDUSTRY CLASSROOM*

SOURCE OF INSTRUCTION: Local Community College, Computer Based Training

Instructor Led Training (ILT)		
Qual Area	Class / Course Title	Hours
Level 1	Security Concepts	40
Level 1	"Information Age Technology" Federal Information Systems Security Awareness" "Computer Security 101", "Protect your AIS", Protect your AIS, the Sequel" "Networks at Risk" "Identity Theft: Protect Yourself" (WBT) Videos	4
Level 1	"Warriors of the Net" (WBT)	1
Level 1	Networking 1	40
Level 1	Networking 2	40
Level 1	Network Security Basics	40
Level 1	Networking 3	40
Level 1	Operations Security Technology	40
Level1	Risk Assessment Basics	40
Level 1	Written Communication	25
Level 1	Oral Communication	40
		350
Level 2	Networking 4	40
Level 2	Internet Firewalls and E-Commerce	40
Level 2	Network Security, Communication & Authentication	40
Level	Network Attacks, Computer Crime & Hacking?	40

2		
Level 2	Security Management Practices	40
Level 2	Incident/Response & Handling	40
Level 2	Security Assessment	40
Level 2	IAM Training	40
Level 2	Human Resources	30
		350
Level 3	Cyber Law	40
Level 3	Design and Development of Instruction Materials and resources	40
Level 3	IT Auditing & Assurance	40
Level 3	Studies in Network Security	40
Level 3	Forensics	40
Level 3	Cryptography	30
Level 3	DB, NW, Web and Wireless Security Issues and Strategies.	40
Level 3	Innovative Thinking	30
Level 3	Strategic Vision	25
Level 3	Risk Management	25
		350

RELATED CERTIFICATION SCHEDULE FOR:
INFORMATION ASSURANCE

METHOD OF DELIVERY: *IN HOUSE TRAINING, COMMUNITY COLLEGE,*

UNIVERSITY, PRIVATE INDUSTRY CLASSROOM

SOURCE OF INSTRUCTION: Local Community College, Computer Based Training

Technician Level 1	Technician Level 2	Technician Level 3
A+ Network+ TICSA SSCP	GSEC Security+	CISSP CISA GSE

Appendix A

INFORMATION ASSURANCE — *DEFINITIONS*

Information Assurance (IA) - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Availability - Assuring information and communications services will be ready for use when expected.

Integrity - Assuring information will not be accidentally or maliciously altered or destroyed.

Authentication - Positively verifying the identity of sender and recipient of data.

Confidentiality - Assuring information will be kept secure, with access limited to appropriate persons.

Non-Repudiation - Assuring that proof of delivery is provided to the sender and proof of sender identity is provided to the recipient, so that neither can later deny having processed the information.

Appendix B

Possible Job Titles for Information Assurance Apprentice Participants

Level 1 - Technician
Computer Security Technician
Information Assurance Tester
Junior Information Security Analyst
Network Defense/Firewall Administration

Level 2 & 3 –Technician
Level 1- Management
Chief Information Systems Security Engineer
COOP Architect/Analyst (Continuity of Operation)
Disaster Recovery Specialist
Information Assurance Analyst
Information Assurance Engineer
Information Assurance Consultant
Information Assurance System Engineer
Information Forensic Engineer
Information Security Engineer
Information System Security Specialist
Information Systems Auditor
Information Systems Security Analyst
Infosecurity Analyst
Infosecurity Engineer
Intrusion Analysis Specialist
Network and Information Assurance Systems Engineer
Network Defense/Firewall Administration
Network Security Engineer
Secure Systems Engineer
Security Analyst
Security Engineer
Security Solutions Architect
Security Specialist
Technical Advisor for Continuity of Operations Support
Wireless Security Engineer

Level 2 & 3 - Management
Computer Systems Security Analysis Manager
Information Assurance Business Development Manager
Information Assurance Security Manager
Information Security Manager
IT Security Program Manager/Business Leader
Network Security Program Manager/Business Lead
Information Assurance Practice Manager
Security Policy Specialist/Manager
Information Assurance Policy Manager
Information Assurance Auditor